Süütu parkimistahvel võib sinu pangakonto hetkega tühjendada

4 kuud tagasi - 05.07.2026 Autor: AM

QR-koodid on kõikjal ja teevad meie elu mugavamaks – alates kohviku menüüde sirvimisest kuni uste avamiseni. Mis juhtub siis, kui see tuttav mustvalge ruudustik, millelt inimsilm siiski sisu välja ei loe, osutub tänavapostil või parkimistahvlil hoopis digitaalseks lõksuks? Eestis on pead tõstmas uus jultunud avalikku ruumi tunginud petuskeem: küberkurjategijad kleebivad parkimismärkidel olevad ametlikud maksekoodid üle oma võltsingutega, suunates kiirustavad ja pahaaimamatud autojuhid õngitsuslehtedele.

Kuidas "pimekood" su kaardiandmed näppab?

Kujuta ette olukorda: oled vihmase ilmaga parklas, sul on kiire ja soovid lihtsalt parkimise eest tasuda. Sa haarad telefoni, skaneerid kähku sildil oleva QR-koodi ning sisestad avanenud lehel oma andmed. Leht näeb välja igati ehtne. Tegelikkuses ei maksnud sa aga parkimise eest, vaid andsid oma raha ning krediitkaardiandmed otse kurjategijatele.

Kuidas see tehniliselt töötab?

QR-koodi puhul on "sihtkoht" sinu silmade eest peidetud – sa ei näe, kuhu see kood sind viib, enne kui oled juba kohal. Tõsi, hoolikamad suudavad ekraanil vilksatavat teadet ehk näha ka, enne kui edasi liiguvad. Kui koodi on teinud pettur, viiakse sind tuttava ja turvalise aadressi asemel hämarasse kangialusesse ehk õngitsuslehele.

Mure on reaalne ning sellele on reageerinud nii parkimisteenuse pakkujad kui ka riiklikud asutused.

Riigi Infosüsteemi Amet (RIA) edastas sotsiaalmeedias tõsise hoiatuse:

> "Ettevaatust! Levimas on parkimismärkidele kleebitud võltside QR-koodide petuskeem. Kuigi QR-kood on väga mugav vahend kasutajate teenuse juurde suunamiseks, kasutatakse seda ka petuskeemides, et pahaaimamatuid kasutajaid rünnata."

Samuti on probleemi ulatust kinnitanud Ühisteenused (Parkimine.ee), jagades juhiseid tekkinud olukorraga toimetulekuks:

> "Oleme saanud teateid, et Ühisteenuste parkimistingimuste siltidele on kleebitud võltsitud QR-koodid, mis suunavad võltsitud makselehtedele. Enne maksmist kontrollige alati, kuhu QR-kood teid suunab. Ühisteenuste ametlikud QR-koodid avavad parkimine.ee ja parkner.ee veebilehed või Parkner mobiilirakenduse."

Kuidas tunda ära petturite lõksu?

Riiklik küberturvalisuse teadlikkuse portaal ITvaatlik rõhutab, et QR-kood iseenesest ei ole pahavara, vaid kõigest infoedastaja. Enamik selliseid rünnakuid toetub sotsiaalsele manipulatsioonile – pettur püüab tekitada sinus hirmu (näiteks parkimistrahvi ees) või kiirustamise tunnet, et sa ei jõuaks loogiliselt mõelda ja veebiaadressi õigsust kontrollida. Parkimise eest tasumisel ongi inimestel tavaliselt kiire ja hirm, et saavad trahvi.

Kõige olulisem nipp on lugeda veebiaadresse. Selle asemel, et lugeda aadressi vasakult paremale, hakka seda lugema veebibrauseri aadressiribal esimesest ühekordsest kaldkriipsust (/) vasakule.

- Õige: aadressi (https://www.eesti.ee/) puhul jääb esimesest kaldkriipsust vasakule domeen eesti.ee. Sa oled õiges kohas!
- Vale: aadressi (https://omniva.ee.popsi7.com/index.php) puhul jääb esimesest kaldkriipsust vasakule popsi7.com. See näitab, et hoolimata "omniva" nimest aadressi alguses asud sa tegelikult petturite loodud popsi7 lehel.

Millistest QR-koodidest peaks eemale hoidma?

ITvaatliku juhiste kohaselt hakkab punane tuluke põlema, kui puutud kokku järgmiste olukordadega.

- Üle kleebitud koodid: see on füüsilises ruumis suurim ohumärk. Kui näed, et originaalsele sildile või plakatile on peale pandud kleeps, on tõenäoliselt tegu pettusega.
- Tundmatu päritoluga kleepsud: ilma igasuguse selgitava tekstita QR-koodid bussipeatustes, liftides või tänavapostidel.
- Liiga hea, et olla tõsi: lubadused stiilis „Võitsid auhinna“, „Tasuta raha / kingitus“ jne.

- Ootamatud andmepäringud: koodid, mis viivad lehtedele, kus nõutakse sinu paroole, PIN-koode või isikukoode tundmatus keskkonnas.
- Kahtlased lühilingid ja domeenid: aadressid, mis lõppevad näiteks .xyz, .click, .ru või tuntud brändide nimed, mis on meelega vigaselt kirjutatud (näiteks faceb00k, go0gle jne). Samuti lühilingid nagu bit.ly, mis ei lase sul eelnevalt lõplikku sihtkohta näha.
- Nõuded midagi alla laadida: lehed, mis sunnivad sind telefoni paigaldama uusi äppe stiilis „Laadi alla see rakendus“ või „Uuenda kohe“.

Kuidas parkimise eest turvaliselt tasuda?

Selleks, et säästa oma närve ja rahakotti, soovitab Parkimine.ee kasutada parkimise eest tasumiseks kontrollitud ja turvalisi kanaleid:

1. Kasuta ametlikku Parkner mobiilirakendust.
2. Mine otse nutiseadme brauseris veebilehele parkimine.ee.
3. Tasuda saab ka vanamoodsal, aga turvalisel moel: saates SMS-i parkimistsooni numbriga lühinumbrile 1902.

Kui märkad linnapildis parkimissildil kahtlast või ilmselgelt üle kleebitud QR-koodi, ära kõhkle – anna sellest kohe ka teenusepakkujale teada.

- Uudised

- Tarkvara
- Turvalisus

Pilt


Tsoon YT12
0,90€/30min
6€/24h
Parkimiseks lae alla Parkner äpp.
For parking please download Parkner app.
Download on the App Store
GET IT ON Google Play
SMS-ga parkimine: saada numbrile 1902 auto reg nr ja tsoon (nt:YT12). Parkimise lõpetamiseks helista numbrile 1903. Parkimise alustamise hind vastavalt mobiilsideoperaatori hinnakirjale. Vajalik Eesti mobiilside-operaatori teenus.